



Qualys Security Conference Dubai

# A 360° Approach to Securing the Cloud

Total Visibility and Comprehensive Security for Cloud workloads and infrastructure

**Hari Srinivasan**

Director Product Management, Qualys, Inc.

# Agenda

Your responsibility in cloud security

Qualys Security for hardening and standardizing workloads

Qualys security for Infrastructure

Qualys security for SaaS

Use Cases & Demo

Q&A



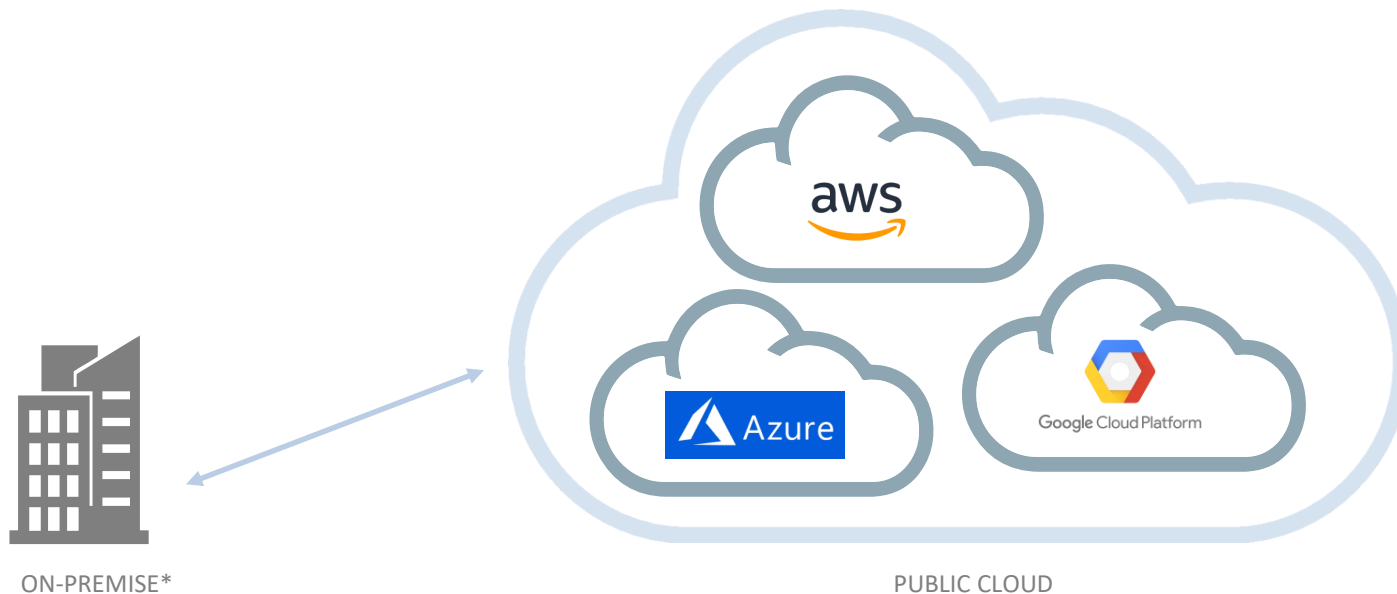
# Customer's landscape is changing

Bahrain Institute of Public Administration  
has moved their Learning Management  
System to AWS, reducing cost by 90%

Bahrain IGA is taking a cloud first policy  
migrating 700 servers with more than 50  
TB data to AWS



# The New IT – Hybrid, Multi-Cloud Deployment



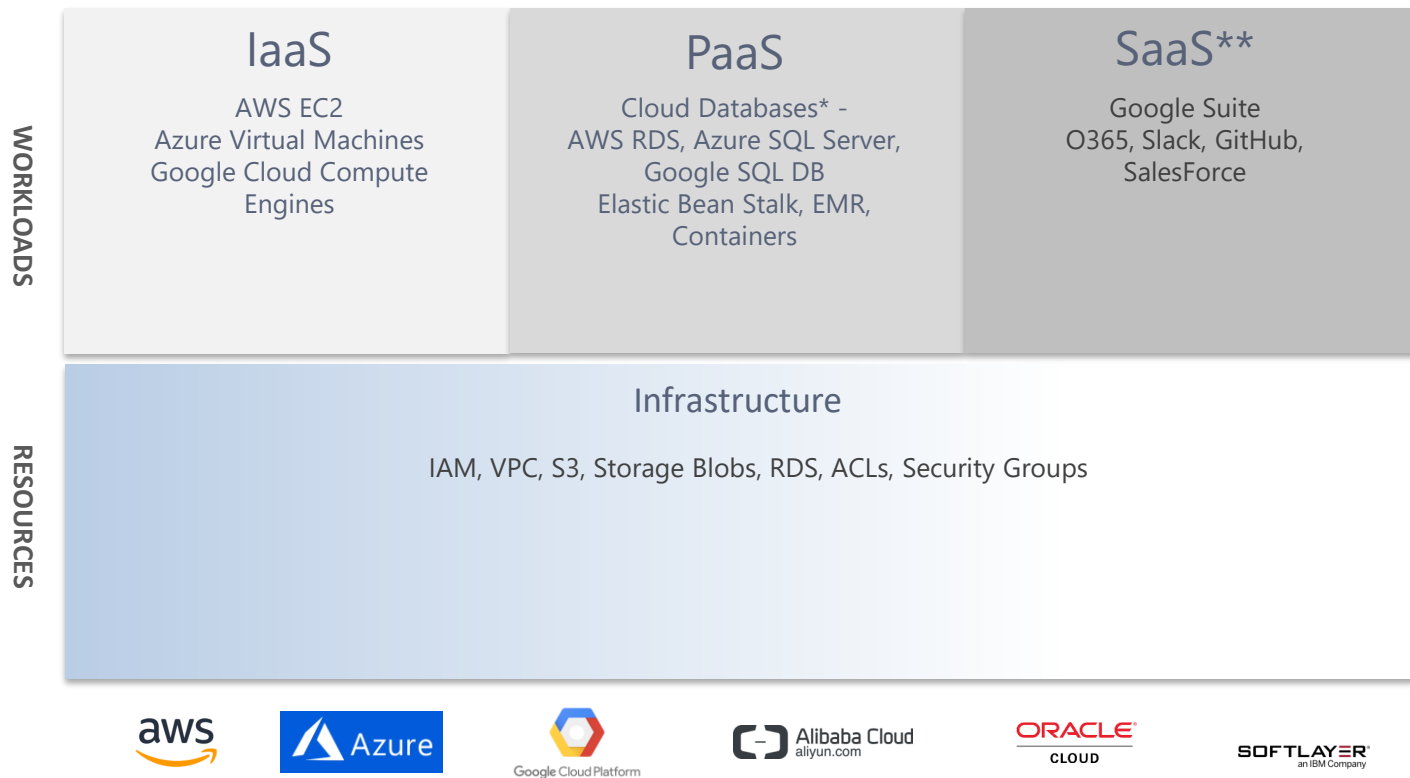
# Shared Security Responsibility Model

# You

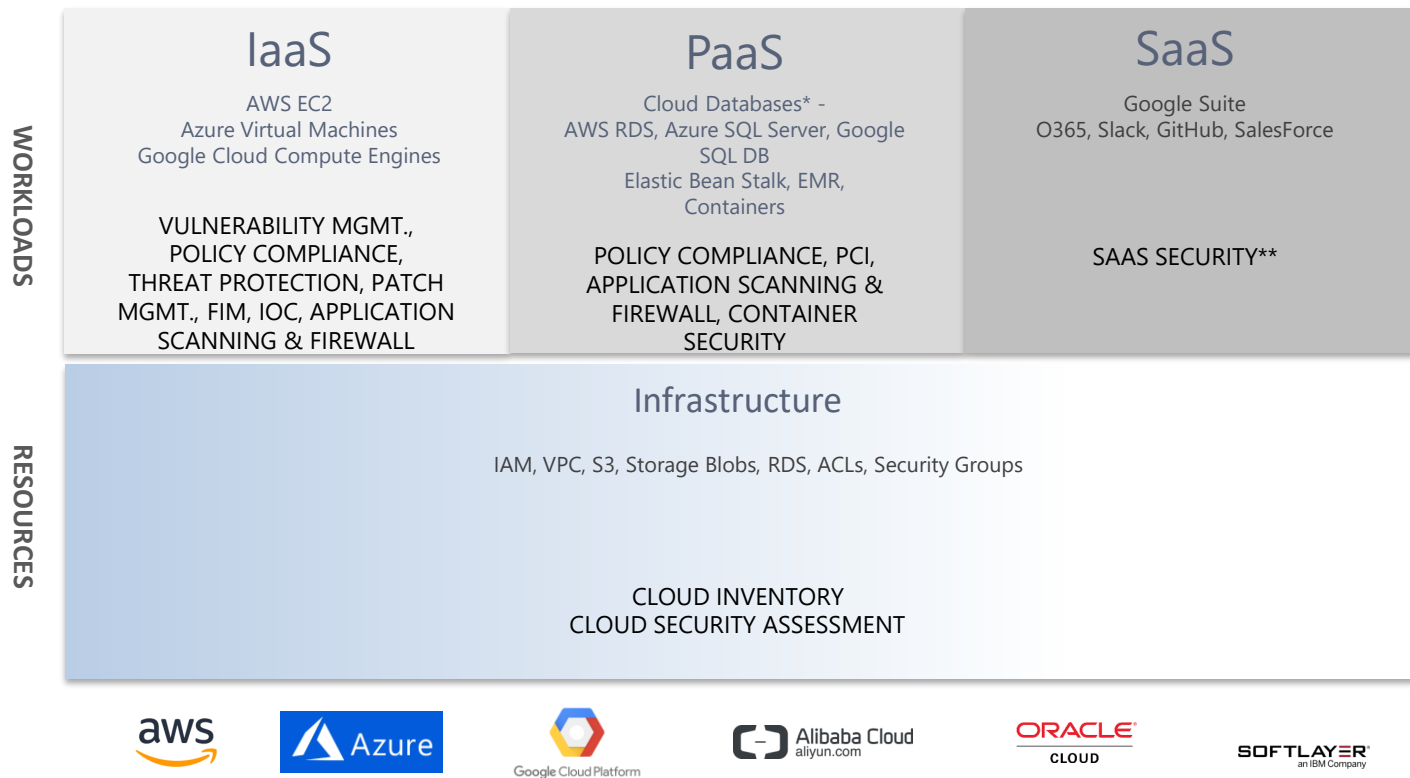
are responsible for securing your data and workloads



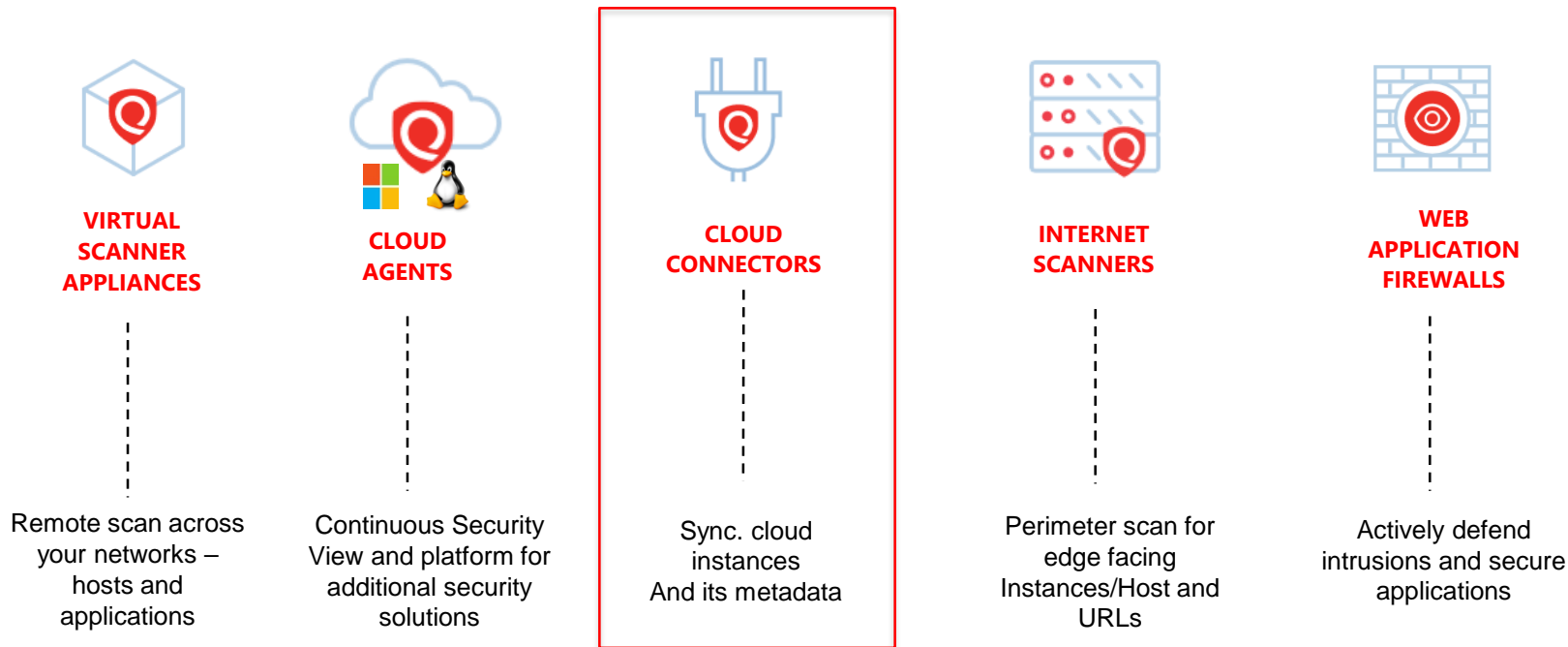
# Components of Cloud Security



# Components of Cloud Security



# Qualys Sensors for Public Clouds



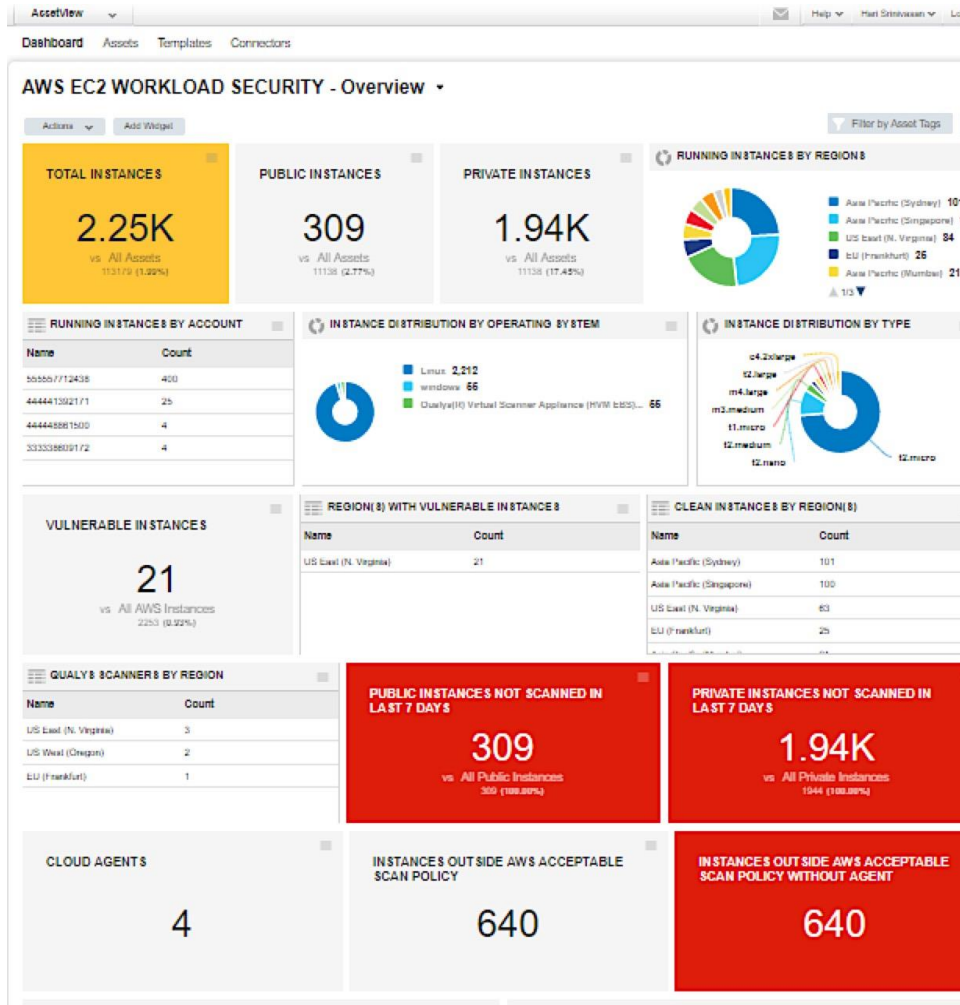


# Cloud Inventory & Security Posture Dashboard

Visibility into your cloud instances inventory

Identify your security coverage

View Security posture



# Cloud Workload Security

# Securing Cloud Workloads

## Hardening and Standardizing



### VULNERABILITY MANAGEMENT

- Vulnerability Management (Internal & Perimeter)
- Threat Protection
- Indicators of Compromise
- Patch Management\*

### POLICY COMPLIANCE

- Policy Compliance (incl. Secure Configuration Assessments)
- File Integrity Monitoring

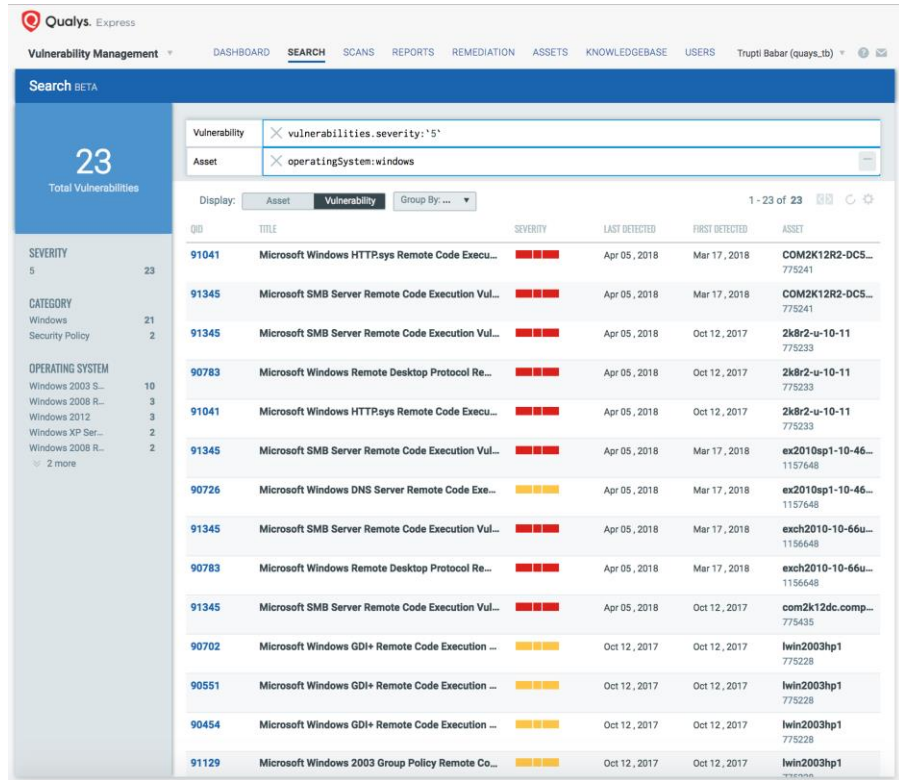
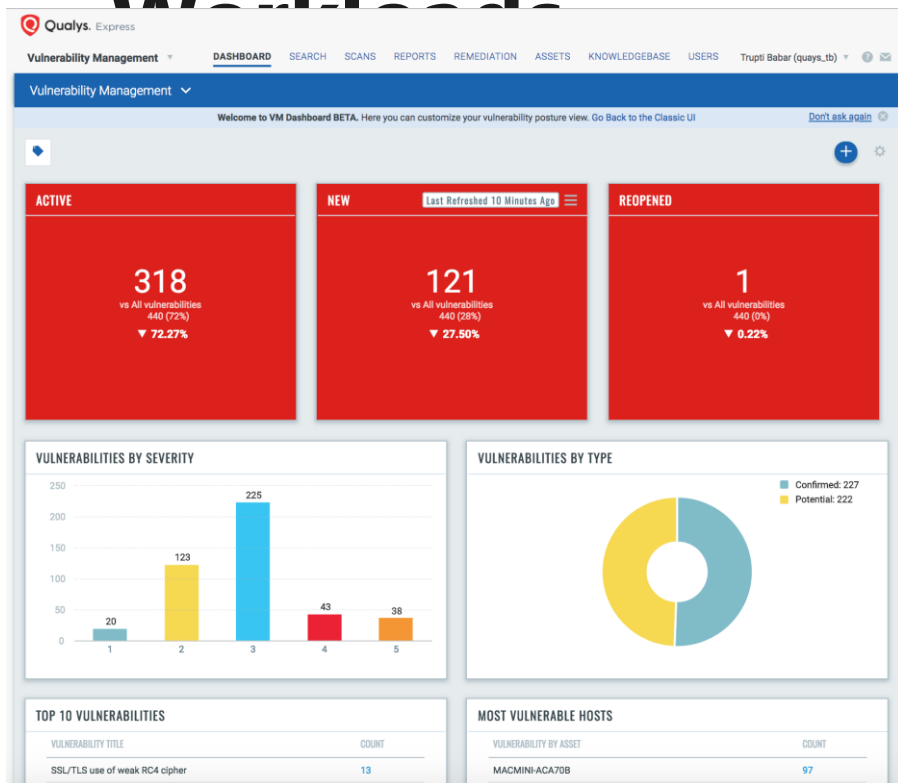
### APPLICATION SECURITY

- Web Application Scanning (WebApps and REST APIs)
- Web Application Firewall

\* Upcoming feature

# Vulnerability Mgmt. for Cloud

## Workload



# Vulnerability Mgmt. - External / Perimeter Workloads

Get a hacker's-eye view of your public  
facing cloud environment

Runs remote check vulnerabilities like  
password brute force, port checks,...

The screenshot displays the Qualys Vulnerability Management interface. At the top, the 'Vulnerability Management' dropdown is visible, followed by navigation tabs: 'Dashboard', 'Scans', 'Reports', and 'Remediation'. The 'Scans' tab is active, showing sub-tabs for 'Scans', 'Maps', and 'Schedules'. Below these, there are buttons for 'Actions (0)', 'New', 'Search', 'Filters', and 'My Scans'. A dropdown menu is open under 'New', listing options: 'Scan', 'EC2 Scan', 'Schedule Scan', 'Schedule EC2 Scan', and 'Cloud Perimeter Scan'. The 'Cloud Perimeter Scan' option is highlighted with a red rectangle. To the right of the interface, red text annotations state: 'Auto selects Public Instances.' and 'Add Load Balancer's DNS'. Below the main interface, a modal window titled 'Launch Cloud Perimeter Scan' is open, showing 'Step 3 of 6' in the process flow. The 'Target Hosts' section includes filters for 'Include hosts that have' and 'Do not include hosts that have', both set to 'Any' of the tags below. There are 'Add Tag' buttons next to each filter. Below these, there is a section for 'Add DNS List (For internet facing ELBs)' with 'Remove Selected', 'Remove All', and 'Add' buttons. At the bottom, there is a text field for 'Assigned Hostnames' and 'Cancel' and 'Continue' buttons.

Vulnerability Management

Dashboard Scans Reports Remediation

Scans Maps Schedules

Actions (0) New Search Filters My Scans

Scan  
EC2 Scan  
Schedule Scan  
Schedule EC2 Scan  
Cloud Perimeter Scan

Host

Launch Cloud Perimeter Scan

Turn help tips: On | Off Launch Help

Step 3 of 6

1 Scan Details  
2 Target Connector  
3 Target Hosts (Optional)  
4 Scheduling (Optional)  
5 Notification (Optional)  
6 Review and Launch

Target Hosts

Filter by Specific Tags

Include hosts that have Any of the tags below Add Tag

No tags selected

Do not include hosts that have Any of the tags below Add Tag

No tags selected

Add DNS List (For internet facing ELBs)

Remove Selected Remove All Add

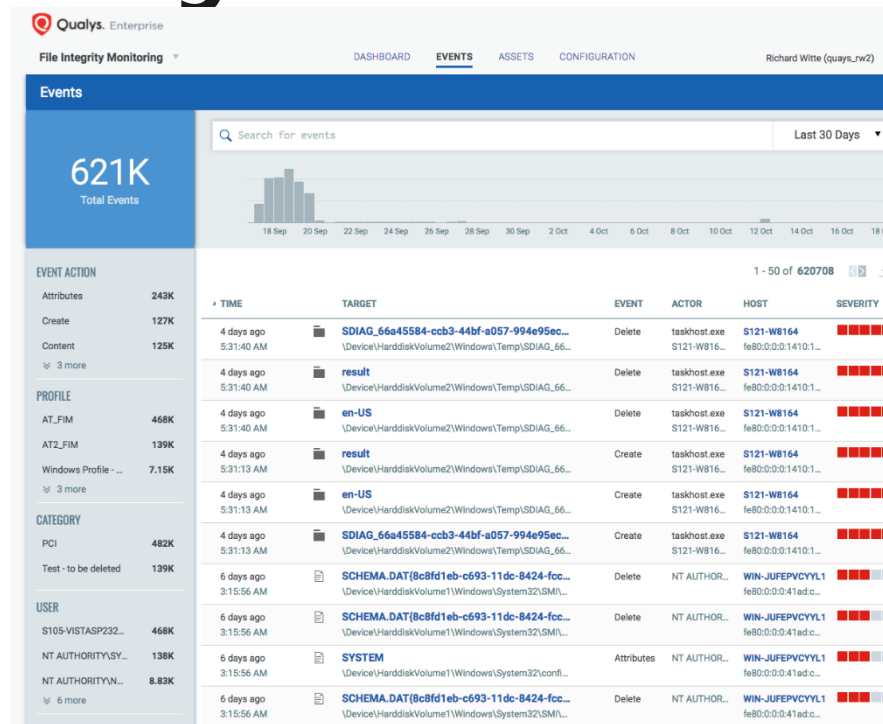
Assigned Hostnames:

Cancel Continue

Auto selects Public Instances.

Add Load Balancer's DNS

# Comprehensive Compliance Management & File Integrity Monitoring



# Moving Toward the Future of Security

Collaborative, Continuous Secure  
Development and Deployment

- ✓ Static Code Analysis
- ✓ Vulnerability Management
- ✓ Compliance Checks
- ✓ Web Application Scanning
- ✓ Configuration Assessments

Comprehensive  
evaluation  
at an early stage  
(DevOps)



# Securing Public Clouds Using Qualys

## Customer Case Studies



Reduced application releases from 2 weeks to 24 hrs by automating security with Qualys in to DevOps

A SOFTWARE  
MAKER

*Private*

"Just in time" security approvals with end to End integration of Qualys Scan and Reports with Service Now,

A BEVERAGE  
MNC

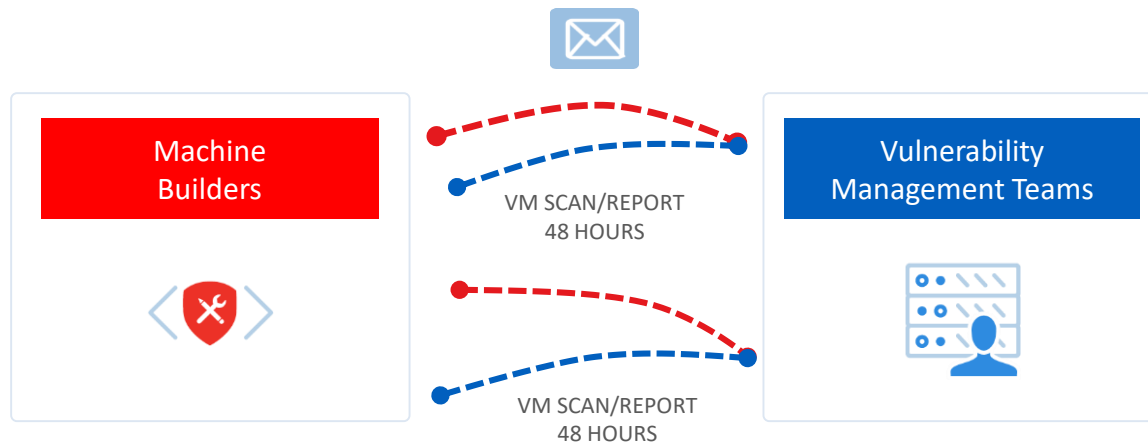
*Private*

Enabling DevOps with automated agent deployment via Azure Security Center



# Capital One

## Before: Lack of Security Automation Delays Release

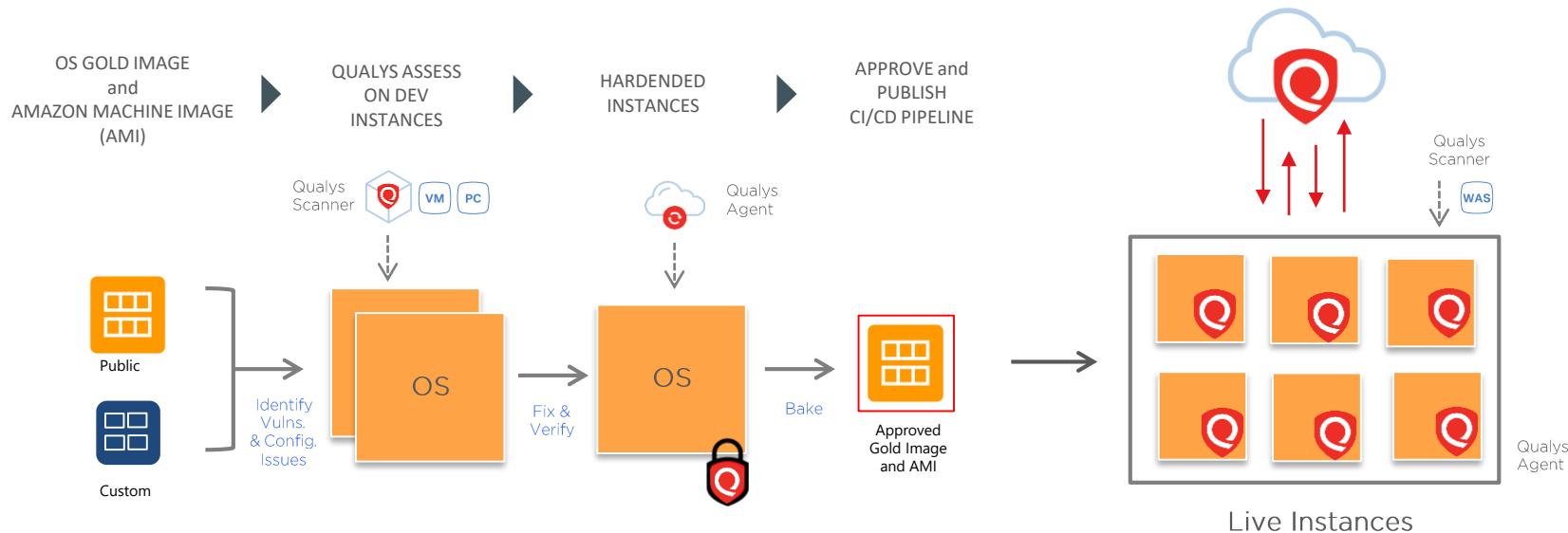


Two weeks until the Image (AMI) is certified for production

# Capital One

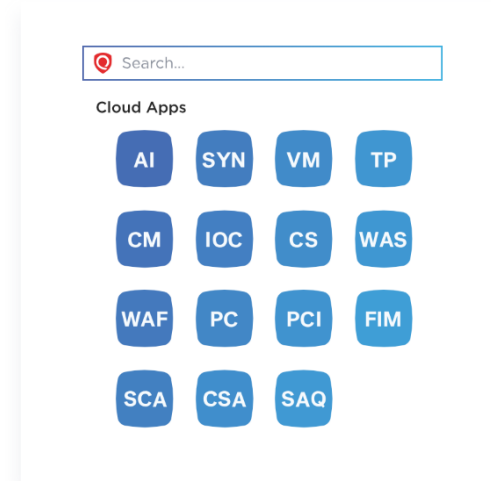
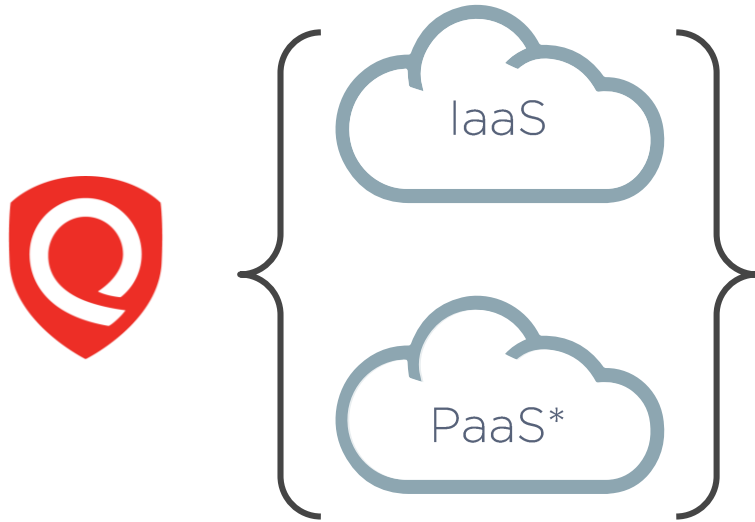
## After: Introducing Security at the Source

Qualys Security into Gold Images and AMI



Bakery process happens within 24 Hrs

# Cloud Workload Security with Qualys



\* PaaS – Cloud Database Scanning – Roadmap 2H '19

# Cloud Infrastructure Security



Australian Insurance Company

# Visibility of deployments stop misuse of keys



AWS sent a notice of compromised keys attempting to create multiple accounts in EU

## Use Case

Identify the resources in EU region, find the Amazon S3 buckets which are open to public and have the keys stored

## Requirement

- Identify where the deployments are located
- Identify Amazon S3 buckets that are public and fix it
- Ensure best practices are followed by IAM users of the account

Company Profile  
Largest provider of Auto and Agriculture insurance

INDUSTRY: Insurance

REGION: Australia

CLOUD:  
Primary Cloud - AWS  
Secondary Cloud- Azure

DEPLOYMENT REGION:  
Australia

SERVICES USED:  
EC2, S3, RDS, EMR, Cloud Front

# Qualys Cloud Inventory and Security

## Assessments

Unparalleled Visibility and  
Continuous Security  
Monitoring across public cloud  
infrastructure



Cloud  
Inventory



Cloud  
Security  
Assessment

## Use Case #1



# Visibility into your public clouds

View into

- Resource Distribution by Type
- Resources by Region

Personalize and add custom widgets



## Use Case #2

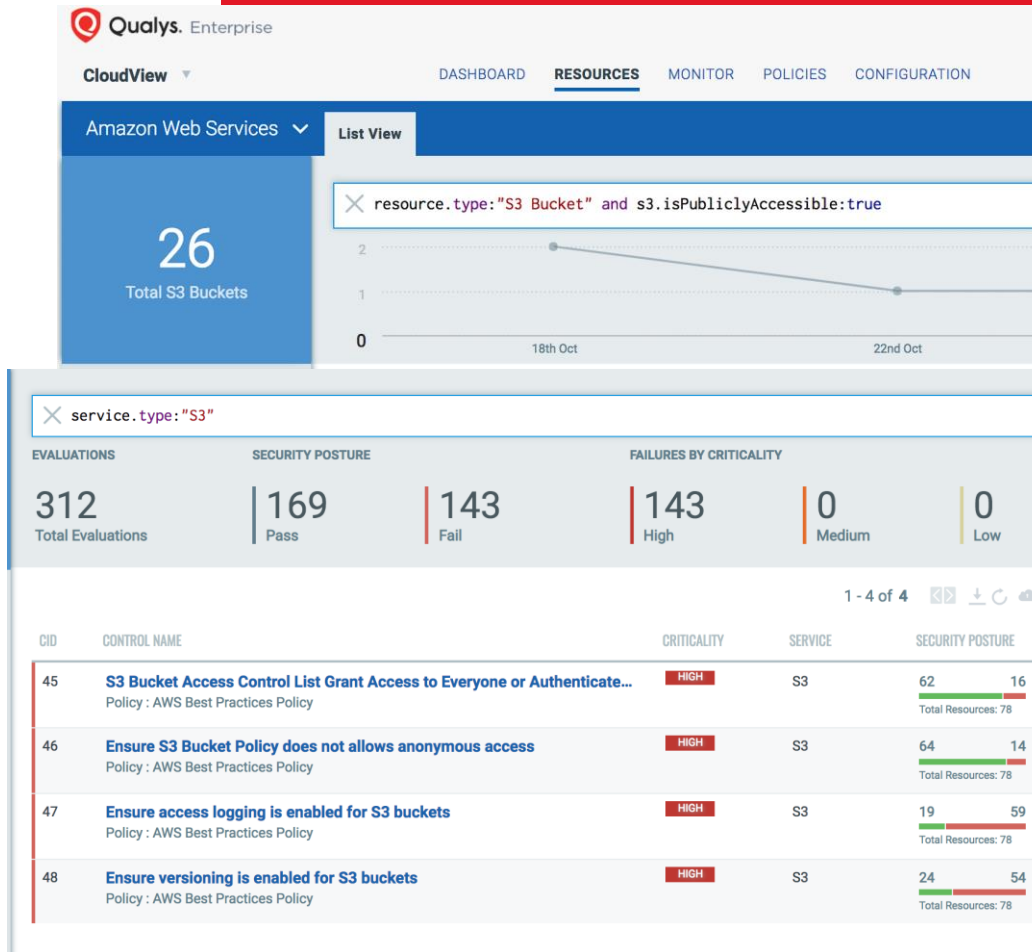


# Identify Leaky S3 buckets

Misconfigured S3 Buckets are vulnerable for data leaks

Check the S3 Bucket Access Permissions Regularly

- Review Access Control List
- Check Bucket Policy





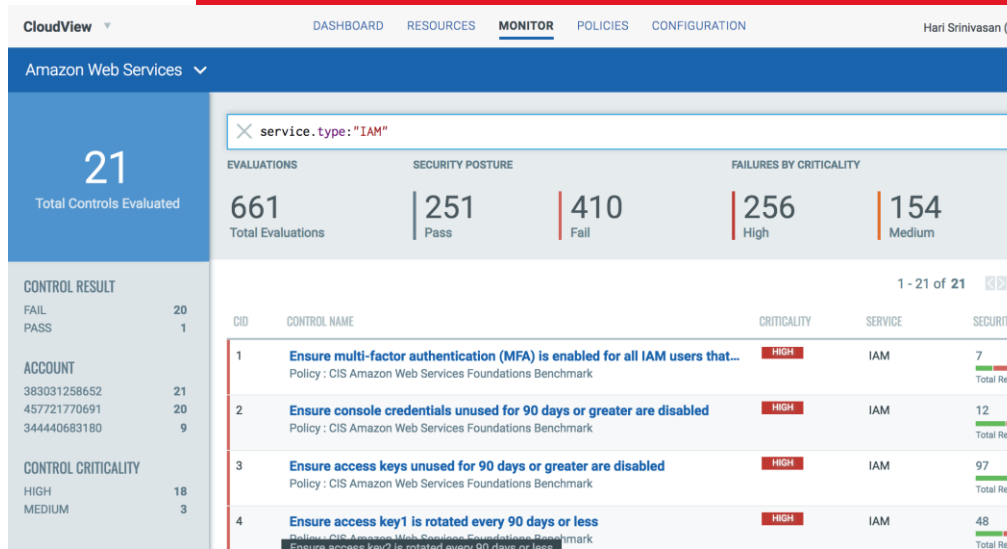
## Use Case #3



# Detect Compromised IAM Users

Check for:

- Configure Strong Password Policy for Account
- Enforce MFA for Console Users
- Rotate IAM Access Keys Every 90 Days
- Removed Unnecessary Credentials
- Audit Process
  - Create separate user for console & API access ( Segregation of duty)
  - Track password age
  - Deactivate unused keys



# Visibility of deployments stop misuse of keys



AWS sent a notice of compromised keys attempting to create multiple accounts in EU


### Requirement

- Identify where the deployments are located
- Identify S3 buckets that are public and fix it
- Ensure best practices are followed by IAM users of the account

### Solution

With Qualys Cloud Inventory and Assessment

- ✓ Gain visibility into the global deployments
- ✓ Identify S3 buckets that are public and required fixing
- ✓ Identify the IAM users and their security posture

Company Profile   
Largest provider of Auto and  
Agriculture insurance

INDUSTRY: Insurance

REGION: Australia

CLOUD:  
Primary Cloud - AWS  
Secondary Cloud- Azure

DEPLOYMENT REGION:  
Australia

SERVICES USED:  
EC2, S3, RDS, EMR, Cloud  
Front



## CloudView

A FREE inventory and monitoring service for your public clouds

\* FREE version is for Cloud Inventory, defaults to 3 accounts per cloud, can be extended further

# Correlate with Vulnerability Data

Identify vulnerable instances associated with the security groups

Reduce effort to pull info to SIEM for correlation

Qualys Enterprise

← Resource Details: sg-08e84245777aa2a62

Summary  
Rules  
Associations  
Tags  
Controls Evaluated

### Associations

Instances ELB Reference Security Groups

1 - 12 of 12

INSTANCE ID	REGION	CREATED ON	STATE	VULNERABILITIES
<a href="#">i-0b0c3f79a6df4ac05</a> AJMdkrh03	N. Virginia	Nov 28, 2018	running	1
<a href="#">i-056756d302b6dbddb</a> AJMdkrh02	N. Virginia	Nov 28, 2018	running	1
<a href="#">i-04b5914b57a4f0055</a> Win2016_Test_SMN	N. Virginia	Nov 28, 2018	running	14
<a href="#">i-09f0a433571db4e0d</a> ssm-Windows2008R2	N. Virginia	Nov 28, 2018	running	0
<a href="#">i-074f89785daa759ad</a> Ubuntu-Test-SMN	N. Virginia	Nov 28, 2018	running	0
<a href="#">i-0b49e28d2d963c228</a> srv2_grp1	N. Virginia	Nov 28, 2018	running	0
<a href="#">i-0f40566c694a67ffb</a> AJMdkrh01	N. Virginia	Nov 28, 2018	running	1

# Cloud Infrastructure Reports

Generate reports for CIS Benchmarks, mandates like PCI, HIPAA, ISO27001, NIST 800-53,..

Configure for specific accounts, and regions

Schedule reports for daily, weekly or monthly

Coming May. 2019

The screenshot displays the Qualys Enterprise CloudView interface. The top navigation bar includes 'DASHBOARD', 'RESOURCES', 'MONITOR', 'REPORTS' (selected), and 'CONFIGURATIONS'. The user 'Dave Jones (qyays\_dj)' is logged in. A search bar is present below the navigation. The main content area shows a list of reports with a 'Quick Actions' menu open for the 'PCI Report for MyAWS Storefront'. The menu options are 'Run Now', 'Download' (highlighted), 'Edit', and 'Delete'. The report details for 'PCI Report for MyAWS Storefront' are shown below:

**REPORT TITLE**  
PCI Report for MyAWS Storefront

**Report Info**

Created date:	05/23/2018 at 00:09:52	Company:	Qualys
Created by:	Hari Srinivasan	Address:	501 The Metropolitan
User name:	qyays_qd		Waldewadi
Role:	Manager		Pune, Maharashtra 411005
			India

**Report Settings**

Policies: CIS Amazon Web Services Foundations Benchmark  
 Asset Selection: All Assets in Policy  
 Template: Payment Card Industry Data Security Standard (PCI - DSS) v3.2

**Report Summary**

Mandates:	Requirements:	PCI - DSS
1	12	96.6%
Connector Name: MyAWS Storefront	Account ID: (383031258652)	
Controls:	Total Evaluations:	Policies:
44	294	1

**Report Statistics**

**Requirement Posture**

Requirement Posture for Payment Card Industry Data Security Standard (PCI - DSS) v3.2

Requirement 1: Install and maintain a firewall configuration to protect cardholder data	100%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	100%
Requirement 3: Protect stored cardholder data	100%
Requirement 4: Encrypt transmission of cardholder data across open, public networks	100%
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs	100%
Requirement 6: Develop and maintain secure systems and applications	100%
Requirement 7: Restrict access to cardholder data to business need-to-know	100%

# Cloud Security Management

Automated remedial actions to protect against risks

End to End flow: Setup On-demand or automated remediation to fix control failures

Scope it by account, controls, tags,..

Coming Q3 2019

Qualys. Express

← Control Evaluation: Ensure console credentials unused for 90 days or ...

### CID-2 Ensure console credentials unused for 90 days or greater are disabled

Policy: CIS Amazon Web Services Foundations Benchmark v1.2.0 - 05-23-2018 Platform: AWS

Evaluation: Check IAM Users having console password and have not used credentials for 90 days or more. Service: IAM

Remediation: [View Steps](#) Criticality: **HIGH**

Search for evaluations

	ACCOUNT ID	EVALUATED ON	RESULT
<input checked="" type="checkbox"/> <b>Actions (50)</b> <b>Remediate Now</b>			
<input checked="" type="checkbox"/> <b>smcvttest</b> arn:aws:iam::383031258652:user/smcvttest	383031258652	18 minutes ago	<b>FAIL</b>
<input checked="" type="checkbox"/> <b>ajoshi@qualys.com</b> arn:aws:iam::383031258652:user/ajoshi@qualys....	383031258652	18 minutes ago	<b>PASS</b>
<input checked="" type="checkbox"/> <b>Mansi</b> arn:aws:iam::383031258652:user/Mansi	383031258652	18 minutes ago	<b>FAIL</b>

# Cloud SaaS Security

# SaaS Security (SSC)

Adya.io now part of Qualys

Manage and Secure your SaaS Applications



Critical SaaS apps



Exposure of Data



For Compliance



On unused Licenses





# SaaS Security and Compliance

## Features

### ADMINISTRATION

- Add /remove users from groups
- Add/ remove users from channels
- Role based access control
- onboarding / offboarding workflows

### SECURITY & COMPLIANCE

- External / internal data exposure
- One click exposure fix
- List / fix dangerous apps
- Alert on exposure / dangerous apps

### LICENCE MANAGEMENT

- Central visibility into SaaS licenses
- See underutilized licenses
- Understand total cost / savings
- Future spend analysis

### REPORT & AUDIT

- Activity logs by user / group
- Access reports for files / folder
- On-demand / scheduled reports
- Pre-built / scheduled reports

10 USERS

22 GROUPS

2002 FILES

1350 FOLDERS



Publicly discoverable Shared public link  
Shared with users outside company Shared across company  
Shared with trusted domain

618 Shared documents

#### External users with most access

neetika@accelero-corp.com	142
deepakbalakrishna@gmail.com	34
dbalakrishna@qualys.com	22
nasar@qualys.com	21
sthakar@qualys.com	21

...and 19 more

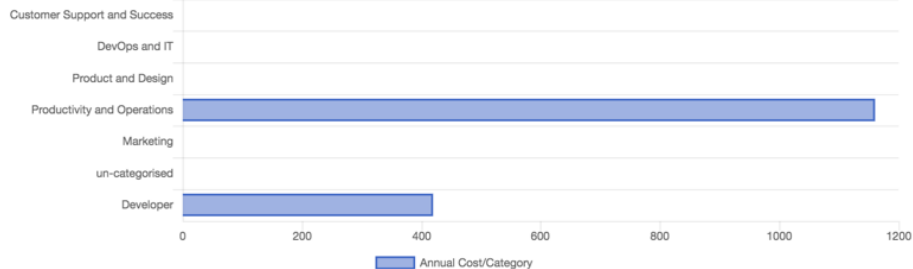
#### Users with most exposed documents

deepak@adya.io	335
scm@adya.io	3
rashmi.singh@adya.io	1

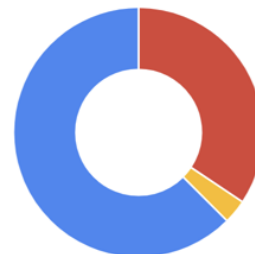


pdf document folder xml mp4  
Others

618 Files Exposed



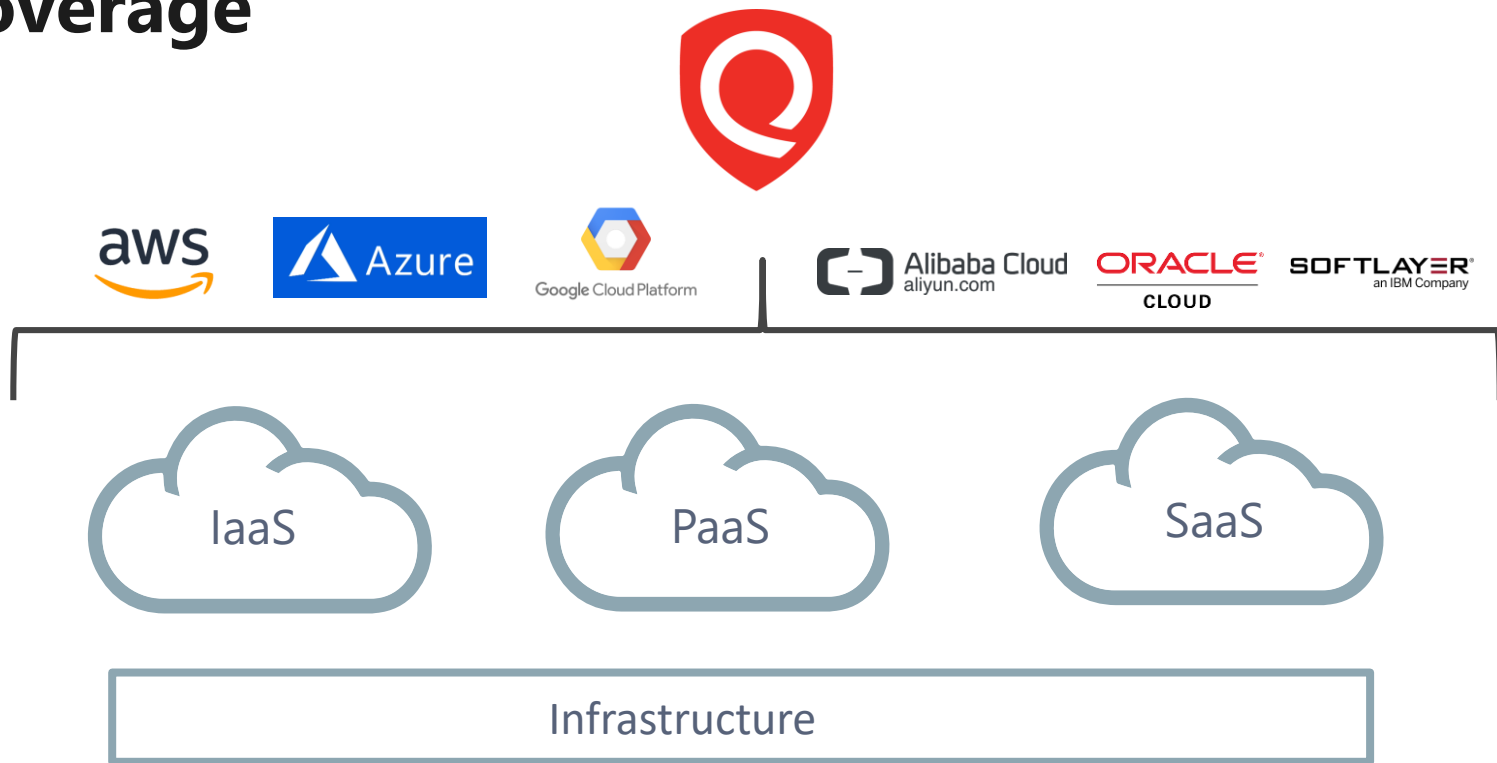
1580.4 \$ in Total Annual Cost



High Risk Medium Risk Low Risk

32 Installed Apps

# Qualys Cloud Security – Comprehensive Coverage



The background of the slide is a complex, repeating pattern of triangles in various shades of blue, ranging from dark navy to light sky blue. The triangles are arranged in a way that creates a sense of depth and movement, with some pointing towards the viewer and others away.

**Q&A**